South Carolina

Law Enforcement Division

NCIC 2000

System Usage Requirements

Version 2.3

January 2004

This document does not constitute a contract and does not alter federal and state law, system regulations, or the user agreements entered into by SLED. The provisions of this document are subject to change at any time by SLED with or without notice or additional consideration. This document is loaned to your agency or organization for authorized purposes only and must be returned upon request.

Table of Contents

APPENDICES

1.0 Introduction

The National Crime Information Center (NCIC) 2000 is the computer system replacing the NCIC System. NCIC 2000 has the same mission and basic functionality as NCIC, but it also features new capabilities described in the NCIC 2000 Operating Manual. NCIC 2000 is a computerized nationwide information system established as a service to all local, state, and federal criminal justice agencies. The goal of the NCIC 2000 system is to help the criminal justice community perform its duties by providing and maintaining a computerized filing system of accurate and timely documented criminal justice information. The criminal justice information, defined in NCIC 2000, is information collected by criminal justice agencies that is needed for the performance of their legally authorized and required functions. This includes:

- Wanted person information
- Missing person information
- Unidentified person information
- Stolen property information
- Criminal history information
- Information compiled in the course of investigating crimes that are known or believed on reasonable grounds to have occurred, including information on identifiable individuals
- Information on identifiable individuals compiled in an effort to anticipate, prevent, or monitor possible criminal activity

The structure and basic procedures of the NCIC System were approved by resolution of the full membership of the International Association of Chiefs of Police in Philadelphia, Pennsylvania in October 1966 and apply to the new NCIC 2000 System. General policy concerning the philosophy, concept, and operational principles of the system is based upon the recommendations of the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) to the Director of the Federal Bureau of Investigations (FBI). The APB is comprised of top administrators from local, state, and federal criminal justice agencies throughout the United States of America. Changes in current applications, addition of new files, and new procedures, such as edits, codes, and validations, are coordinated with all NCIC and NCIC 2000 participants through the advisory board. The Control Terminal Officer (CTO) and a local representative are members of the Southern Working Group.

The NCIC 2000 System stores vast amounts of criminal justice information that can be instantly retrieved by and/or furnished to any authorized agency.

The NCIC 2000 System makes centralized crime data immediately available to the criminal justice community. The success of the system depends on the extent to which patrol officers, investigators, judges, prosecutors, correction officers, and other criminal justice agency officials intelligently use it in day-to-day operations.

The NCIC 2000 System serves local, state, and federal criminal justice agencies in the 50 states, the District of Columbia, Puerto Rico, and Canada. The NCIC 2000 System has become available for use by all criminal justice agencies through established state computer systems.

1.1 System Functionality

NCIC 2000 provides virtually uninterrupted operation 24 hours a day, 7 days a week.

Most records are placed directly into the NCIC 2000 System by an originating agency through a control site (SLED) tied into the network (NCIC). The communication lines and associated costs from the NCIC 2000 computer to SLED are borne by the FBI. The cost of communications between the control terminal agency (SLED) and the point of presence for each regional latta is borne by SLED. SLED also pays for the hardware / software for the Law Enforcement Message Switch (LEMS), the central network and databases infrastructure for NCIC and related networks, such as the National Law Enforcement Telecommunications System (NLETS), training, auditing, and technical support staff. The regional lattas are as follow: Anderson, Augusta (GA), Charleston, Charlotte (NC), Columbia, Florence, Greenville, Savannah (GA), and Spartanburg. The agency interface costs to SLED are borne by the individual agency. There are a few different options to interface with SLED, depending on the frequency of needed access to the NCIC 2000 System.

The FBI NCIC 2000 System and SLED Network computer equipment can interface with equipment manufactured by many of the major computer and communications firms. System participants are not required to use the same make of computer equipment as that used by the FBI and SLED, but certain minimal system configurations are required.

The FBI and SLED use hardware and software controls to help ensure system security. The final responsibility for the maintenance of the security and confidentiality of criminal justice information rests with the individual agencies participating in the use of the NCIC System. The data stored in the NCIC 2000 System and the Interstate Identification Index (III) file are documented criminal justice information and must be protected to ensure correct, legal, and efficient dissemination and use. It is important that an agency, operating a NCIC 2000 device, to implement the necessary procedures to make that device secure from any unauthorized use. Departure from this responsibility may result in sanctions, including termination of system access.

1.2 System Usage

Complete, accurate, and timely records are essential to ensure the NCIC 2000 System integrity. Users are encouraged to enter records in a timely manner to afford the maximum protection to the law enforcement officers and citizens. Delayed entry of records to the NCIC 2000 System reduces or eliminates the possibility of apprehending wanted persons, locating missing persons, and recovering stolen property. Promptness in modifying, locating, or clearing records in the system will help to keep the system free of outdated information.

When an agency receives a positive response from the NCIC 2000 System and an individual is being detained or a piece of property can be seized, an immediate confirmation with the agency that originated the record in the system is necessary. This confirmation ensures the validity of the hit before an arrest or seizure is made. The originating agency has the duty to respond promptly with the necessary confirmation and other pertinent details.

NCIC 2000 provides information for decision-making by investigators, patrol officers, judges, prosecutors, and corrections officials. The information furnished by NCIC 2000 must be evaluated along with other facts known to the officers, investigators, judges, prosecutors, and correction officials.

2.0 NCIC 2000 – SLED Security

NCIC 2000 System information security is based on the concept that access to the NCIC 2000 System is generally limited to criminal justice purposes. The NCIC 2000 System must be safeguarded from all threats of unauthorized access. Technical security and personnel security procedures are intended to prevent potential threats from becoming actual threats. While all threats cannot be identified, basic network architecture and the use of appropriate technology will provide reasonable security. An interface to the SLED computer network must follow an approved design.

A single personal computer with an NCIC 2000 interface, via the Internet, must be designed to include adequate security for state and national systems with which it connects. It is not sufficient to use policy to protect NCIC 2000 access through the Internet since unauthorized access to the personal computer may be achieved through the Internet service provider. There must be an approved personal firewall, encryption software, and anti-virus software installed on the personal computer for security against destructive access to the personal computer, SLED, and the NCIC 2000 System.

A local area network (LAN) with an NCIC 2000 interface, via the Intranet, must be designed to include adequate security for state and national systems with which it connects. SLED provides for encryption from their network to the organization's router. The organization may be required to further encrypt the data between their router and each workstation if those workstations are not solely dedicated to criminal justice or have access to non-criminal justice networks. It is not sufficient to use policy to restrict criminal justice information to authorized personnel when non-criminal justice personnel also use the LAN unless the network is encrypted to the device employed by the end user. If the LAN has any other interface, including the Internet, there must also be an approved firewall installed for security against destructive access to SLED and the NCIC 2000 System.

3.0 Network Connectivity

The NCIC 2000 Law Enforcement Message Switch (LEMS) enables compliance with NCIC 2000 requirements by facilitating the connection between SLED and the FBI. Unisys Corporation is the primary contractor for installation and maintenance of the NCIC 2000 switch in South Carolina. The migration of current users to NCIC 2000 must be completed by December 31, 2003. All users, whether new NCIC users or current users must meet this requirement for NCIC 2000 connectivity.

There are three types of NCIC 2000 configurations being supported by SLED. Each configuration is a compromise between cost and performance.

Internet Inquiry Only Client: This solution allows connectivity to the NCIC 2000 System through the **Internet** and is recommended for light volume access. This solution is supported by SLED with its LEMS.WEB browser-based application. Similar functionally may be available from 3rd party vendors.

Intranet Inquiry or Full Function Client: This is an inquiry only or full function solution supported by SLED. It allows connectivity to the NCIC 2000 System through the SLED **Intranet.** Performance and system response may be more reliable than those using the public Internet. SLED's LEMS.WEB may be used for Inquiry Only. Full function will require use of a SLED approved 3rd party vendor. The using agency will be responsible for purchasing such a vendor product or service.

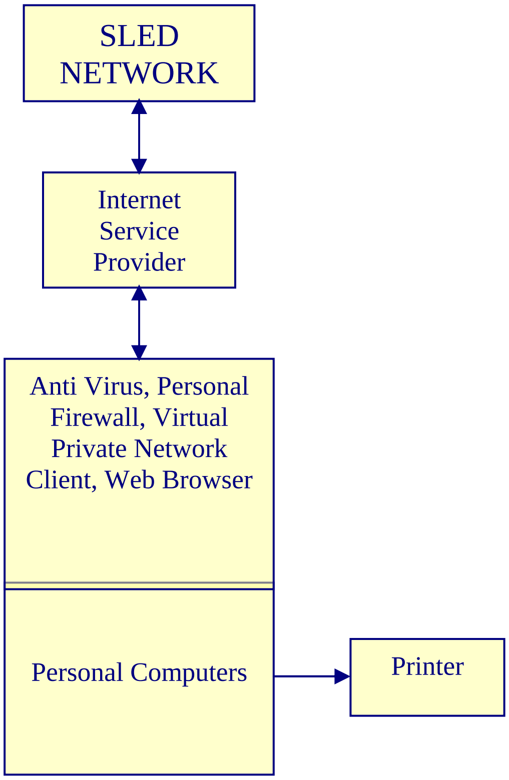
Foreign Host Interface: This is a full function vendor or agency provided solution. It allows connectivity to the NCIC 2000 System through the SLED **Intranet.** Only SLED approved vendors or agencies with appropriate NCIC experience are authorized to develop and operate their product/service on the SLED CJIS network. This solution is recommended where integration with other agency applications, such as a Records Management System, can justify the additional cost and support requirements of it.

The changes in network architecture require that network users make technology-based business decisions not previously addressed. Hardware, software, method of connectivity, maintenance, security, and bandwidth are all issues that must be addressed by users that connect to SCIC/NCIC. Users should consider present and future network usage configuration requirements when making these business decisions. Network members are financially responsible for all NCIC 2000 related costs as they migrate to TCP/IP.

4.0 Network Specifications

Agency connectivity to the NCIC 2000 System, through the SLED Network, requires certain minimal hardware configurations. The Justice Communications staff at SLED have analyzed and upgraded the SLED Network to accommodate agency access to the NCIC 2000 System. This network requires a certain level of hardware performance from the user community as well. The technicians have developed the following system schematics and specifications to assist you in determining your hardware requirements and configurations. Your hardware requirements are partially based on your access needs. Please do not order any hardware or telecommunication lines without first consulting with the SLED IT staff to determine your needs and security requirements.

4.1 Internet Inquiry Only Client Access


SLED NETWORK
Internet Service Provider
Anti Virus, Personal Firewall, Virtual Private Network Client, Web Browser
Personal Computers
Printer

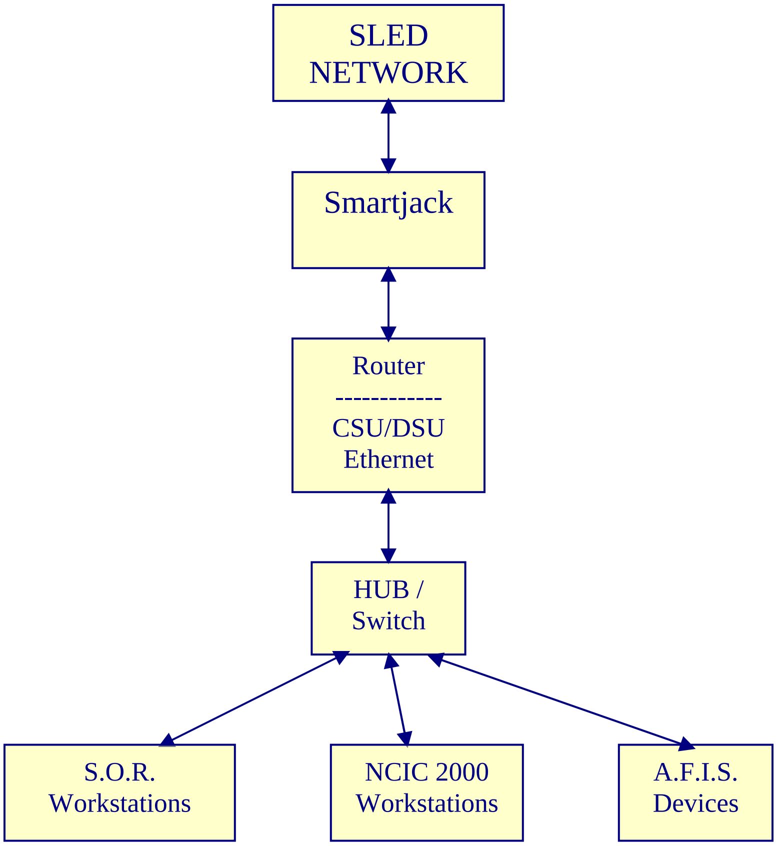
The Inquiry Only Client configuration uses the Internet and a web browser to access the NCIC 2000 System. Your hardware and software requirements to use the NCIC 2000 System via the Internet are:

Personal Computers

RECOMMENDED HARDWARE	RECOMMENDED SPECIFICATIONS
Processor	1.6 GHz with 128k Cache Memory
Memory	512 Megabytes SDRAM
Monitor	17 inch color monitor
Hard Drive	30 Gigabytes
Sound System	Integrated sound card and low cost external speakers
Network Adapter	10/100 Ethernet
Operating System	Windows 2000 or XP
Web Browser	Internet Explorer version 5.5 or higher
Other Hardware	Keyboard, mouse 3.5 inch floppy disk drive, CD-ROM drive
Other Software	Anti-virus, personal firewall, VPN client (SLED supplied)

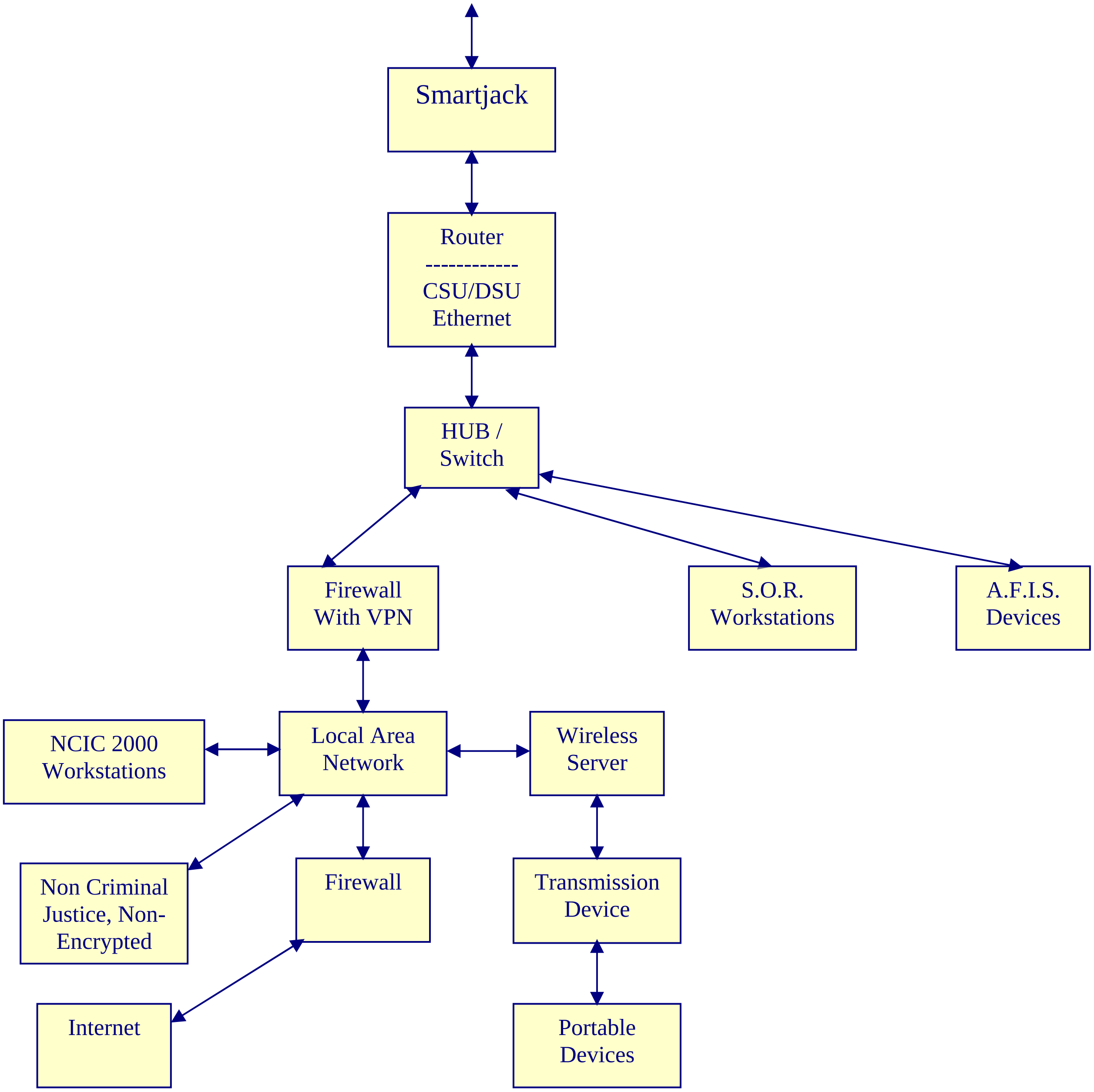
MINIMUM HARDWARE	MINIMUM SPECIFICATIONS
Processor	1.2 MHz
Memory	256 Megabytes SDRAM
Monitor	15 inch color monitor
Hard Drive	20 Gigabytes
Sound System	Integrated sound card and low cost external speakers
Network Adapter	10/100 Ethernet
Operating System	Windows 2000 or XP
Web Browser	Internet Explorer version 5.5 or higher
Other Hardware	Keyboard, mouse 3.5 inch floppy disk drive, CD-ROM drive
Other Software	Anti-virus, personal firewall, VPN client (SLED supplied)

4.2 Full Functionality Client Access via SLED’s CJIS Network



Notes:

Configuration is dedicated to criminal justice
No Internet connection
No connections to non-criminal justice networks
No modems
No requirement for VPN to individual workstations or devices



Notes:

Not dedicated to criminal justice
Internet access
VPN required to NCIC 2000 workstations

ATM frame relay is the recommended line access to the SLED Network when connecting to the NCIC 2000 System. It offers the best performance and reliability option.

You have the option of selecting either a T-1 or 64K-line to access the SLED Network. You will achieve better performance and response with a T-1 line, but a 64k line is currently a little less expensive. When determining required line speed, consider other uses that can also be made of the line. For example, a Sex Offender Workstation can share a 64K line with several NCIC 2000 PCs. However, if an AFIS device or other image application is present, a T1 line will be needed to handle the increased data while keeping the NCIC transaction response times within an acceptable limit. In addition, to save money you should consider sharing the line with other agencies whenever possible.

The Full Functionality Client configuration uses the intranet to access the NCIC 2000 System. Agencies wishing to employ a vendor provided client configuration should contact SLED CJIS for information regarding an approved provider.

Your hardware and software requirements to use the NCIC 2000 System via the intranet are:

HARDWARE	PROVIDER
Frame Relay	OIR/BellSouth/SCNet

Router

CSU/DSU
Ethernet

PART NUMBER	DESCRIPTION
CISCO2610XM	10/100 Ethernet Router w/ Cisco IOS IP
S26C-12301	Cisco 2600 Series IOS IP
MEM2600XM-32U48FS	32 to 48MB Flash Factory Upgrade for the Cisco 2600XM
Select one of the following Interface Card Options	
WIC-1DSU-T1	1-port 4-WIRE T-1 WAN Interface Card
WIC-IDSU-56K4	1-port 4-WIRE 56/64 KBPS WAN Interface Card
NOTE: Do not order Cisco SmartNet maintenance. All maintenance and support will be provided by the Office of the CIO and you will be billed directly by them.	

A list of vendors soliciting CISCO products for networking systems and approved on the state contract can be found at http://cio.state.sc.us/itmo/contract/itsclist.htm.

HUB /
Switch

HARDWARE	OPTIMUM SPECIFICATIONS
Hub / Switch	High quality managed 10/100 auto-sensing switch with 12 or more ports

HARDWARE	MINIMUM SPECIFICATIONS
Hub / Switch	Quality unmanaged 10/100 auto-sensing switch with 8 or more ports

Firewall

Networks that have terminals accessing CJIS and/or the Internet (e.g., peer-to-peer relationships and large mainframes/servers that house web sites) must be protected by a firewall. These firewall devices must implement the minimum firewall profile guidelines of providing a point of defense and a controlled and audited access to servers, both from inside and outside the CJIS networks.

Neither the FBI CJIS nor SLED mandates that a particular firewall type or brand be used. Use of the U.S. Government Application Level Firewall Protection Profile for Low Risk Environments and U.S. Government Traffic Filter Firewall Protection Profile for Low Risk Environments is recommended. Traffic filter firewalls should have the ability to screen traffic at the network and transport protocol layers and to audit related events.

Application level firewalls should provide the capability to screen traffic at the application protocol layer, in addition to the network and transport layers, as well as the ability to authenticate end users with additional audit capability. The protection profiles define the functional characteristics of firewalls without specifying particular vendors and equipment. Firewalls that provide all of the specified security features and assurances can be evaluated against the profiles to determine compliance. The profiles effectively show the relationship between the technical controls and the associated operational considerations (e.g., physical security, configuration management, audit review). The profiles are available upon request from the FBI. Both profiles and additional information can also be found at http://www.iatf.net/protection_profiles/firewalls.cfm.

Personal Computers

RECOMMENDED HARDWARE	RECOMMENDED SPECIFICATIONS
Processor	1.6GHz with 128k Cache Memory
Memory	512 Megabytes SDRAM
Monitor	17 inch color monitor
Hard Drive	30 Gigabytes
Sound System	Integrated sound card and external speakers
Network Adapter	10/100 Ethernet
Operating System	Windows 2000 or XP
Web Browser	Internet Explorer version 5.5 or higher
Other Hardware	Keyboard, mouse 3.5 inch floppy disk drive, CD-ROM drive
Other Software	Anti-virus
	VPN client (if required), personal firewall (if required)

MINIMUM HARDWARE	MINIMUM SPECIFICATIONS
Processor	1.2 MHz
Memory	256 Megabytes SDRAM
Monitor	15 inch color monitor
Hard Drive	10 Gigabytes
Sound System	Integrated sound card and low cost external speakers
Network Adapter	10/100 Ethernet
Operating System	Windows 2000 or XP
Web Browser	Internet Explorer version 5.5 or higher
Other Hardware	Keyboard, mouse 3.5 inch floppy disk drive, CD-ROM drive
Other Software	Anti-virus
	VPN client (if required), personal firewall (if required)

5.0 NCIC 2000 Instruction and Certification

Every NCIC 2000 System Operator is required to participate in NCIC 2000 training and testing in order to assure compliance with FBI CJIS policy and regulations relating to the use of the NCIC 2000 Computer System. Each operator is also required to participate in NCIC 2000 training and testing biennially to reaffirm their proficiency in the use of the NCIC 2000 System and to assure their compliance with FBI CJIS policies.

There are three certification programs being offered by SLED CJIS to achieve NCIC 2000 certification. The certification program an operator must participate in is dependent on the level of functionality they have to the NCIC 2000 System.

- **CJIS-NCIC 16-Hour Certification –** This level of certification is for operators who have limited functionality access to the NCIC 2000 System. This covers inquiry only access and may be used for wireless and Internet applications.

- **CJIS-NCIC 40-Hour Certification –** This level of certification is for operators who have full functionality access to the NCIC 2000 System. This instruction includes entering files, validating records, and hit confirmation response and inquiries.

- **CJIS-NCIC Instructor Certification –** This “Train the Trainer” course is only available to selected NCIC 2000 System Operators who have been selected by their agency and the SLED CJIS Training Group to teach SLED CJIS-NCIC courses. Participating in and passing the South Carolina Criminal Justice Academy’s ‘Specific Skills Course’ is a prerequisite to this course.

An organization must fill out a Security Profile Form and two ‘blue’ fingerprint cards from the perspective NCIC 2000 System Operator. The Security Profile Form must be notarized and signed by the organization’s Chief Executive Officer or the person representing the C.E.O.

An organization must fill out a Terminal Operator Add/Modify/Delete Form to add, modify, or delete a certified NCIC 2000 System Operator to/from accessing the NCIC 2000 System.

Please refer to the NCIC 2000 Operating Manual for specific information and procedures for obtaining NCIC 2000 training and certification.

6.0 Agency Support and Maintenance

The support and maintenance of hardware and software systems is important to maintain a quality system. SLED will continue to support and maintain quality systems for NCIC access. It is important for the user agencies to maintain the functionality and security of their systems for optimum performance and reliability. Please call the SLED helpdesk when you have a system connectivity to SLED concern. SLED will analyze their systems to determine if the concern is related to their systems. SLED will maintain the central site/systems and pay for the communications backbone for the network. All individual agencies are responsible for maintaining their portions of the system. Agencies not understanding or unable to remedy their system problems are advised to contact SLED. The cost of vendor services to solve agency system problems is the responsibility of the individual agencies.

SLED has negotiated with the Office of the CIO to provide state-wide WAN installation and maintenance assistance. Such support includes the configuration, installation and support of agency routers, 24x7 line monitoring, helpdesk assistance, and rapid diagnosis and repair of failing components. Your agency will be billed directly by the CIO office for any associated charges. You should not order any Cisco SmartNet maintenance since that coverage will be provided by the CIO Office.

7.0 Network Connectivity Procedure

Access to the NCIC 2000 Computer System is achieved through the SLED CJIS network. The following procedure is a structured process for achieving access to the SLED CJIS network. The Network Connectivity Checklist, located in the appendices, may offer some organization to your connectivity process.

1. Send a letter to the Control Terminal Officer (CTO) to request connectivity to the SLED CJIS network.

   The SLED CJIS Connectivity Request Letter should be written to include:

   - Your O.R.I. number. Please note in the letter if you do not have an O.R.I. number.

   - All agencies that have an informational dependency on your access to the SLED CJIS network. Please note in the letter if you have no dependant agencies.

   - Who will be using the connectivity

   - What type of connectivity access is being requested
     Inquiry Only Client
     Full Functionality Client
     Vendor Provided Foreign Host Interface

   - Where the connectivity will occur from

   - When connectivity should begin

   The letter should be addressed to:

   Control Terminal Officer
   SLED CJIS
   P. O. Box 21398
   Columbia, South Carolina 29221-1398

   The letter may also be sent to SLED CJIS via FAX at (803) 896-7244 or via email to cjis_admin@mail.sled.state.sc.us.

2. Shortly after reception of your SLED CJIS Connectivity Request Letter, you will be mailed a collection of informational documentation and several forms for you to complete. The forms mailed to you are dependent on the information you provided in the Connectivity Request Letter. Please fill them out and return them to the same address used for the Connectivity Request Letter. You may receive any or all of the following:

- South Carolina Law Enforcement Division Criminal Justice Information System User Agreement and System Responsibilities Form
- South Carolina Law Enforcement Division Management Control Agreement Form
- Serviced Agency Addendum
- SLED CJIS Site Survey
- SLED CJIS Service Request
- Vendor Interfacing to SLED CJIS Systems
- FBI CJIS Security Addendum
- FBI CJIS Security Policy
- South Carolina Law Enforcement Division NCIC 2000 System Usage Requirements

Please fill out the information requested and return them to SLED. Pay particular attention to the requirement in the Site Survey for a diagram showing what your anticipated configuration will look like. SLED's Information Security Officer (ISO) will review this document to insure proper security safeguards are in place. SLED's technical communications staff will also review the Site Survey to insure your planned installation follows established connectivity guidelines. You may be contacted for clarification or assistance with your request. Your request for line installation and NCIC 2000 connectivity will be delayed until the Site Survey is complete and approved.

3. Establish service provider for Internet or frame relay access

   Once your design is approved, you will be given written notice to proceed. Depending upon your connection requirements, SLED may arrange for the communication lines to be installed or you will contract with an Internet Service Provider. (Refer to the Network Specifications section of this document.)

   If it is determined that your access will be the Full Functionality Client via the intranet, consider the following when establishing your frame relay service:

   - You should consider a T-1 line for access to SLED CJIS if optimal speed is required when accessing NCIC and SLED information. A T-1 line may also be required if you have other devices connected to the network.

- You should consider a 64k-line for access to SLED CJIS if optimum speed is not necessary and cost is a major issue.

4. Procure network and computer hardware and software. The Statement of Work will indicate what hardware and software you will be required to purchase. Information regarding required hardware and software services can be found in the Network Specifications section of this document.

5. Acquire NCIC 2000 instruction and certification for operators.

   Every operator is required to participate in NCIC 2000 training and testing before they are permitted to use the NCIC 2000 System. Registration for this training course is required. (Refer to the NCIC 2000 Instruction and Certification Section of this document)

6. Deliver router to SLED CJIS for configuration.

   Your router needs to be configured by a state CIO network technician before it can be used to interface with the SLED CJIS network. Complete a *Router Configuration Request Form*, located in the appendix, and arrange for the router to be delivered to the following address:

   Information Technology Officer
   SLED CJIS
   4400 Broad River Road
   Columbia, South Carolina 29210

7. Install and test hardware at your organization.

   A state CIO representative will configure and schedule the installation of the router at the originating organization's site and verify its connectivity to the SLED CJIS network. Any other hardware set up at the organization's site is the operational and financial responsibility of the organization.

Appendix A - Network Connectivity Checklist

This checklist has been created to assist an organization in determining what to do and when to do it to gain access to the NCIC 2000 System. These procedures should be followed in top/down order. Check off the procedures when you have completed their requirements.

□ Send a letter to the CTO to request connectivity to the SLED CJIS network.

□ Complete and return the Site Survey and any other documentation required. Work with SLED's technical support staff and Information Security Officer to resolve hardware, connectivity, security, and service provider options.

□ Establish service provider for Internet access

□ Procure network and computer hardware and software

□ Acquire NCIC 2000 instruction and certification

□ Complete a *Router Configuration Request Form* and deliver the router to SLED CJIS for configuration by the Office of the CIO

□ Install and test hardware

Appendix B

Vendor Interfacing to SLED CJIS Systems

1. A signed request must be received from a sponsoring law enforcement agency. This letter must contain a statement of what the agency wants the vendor to accomplish, what hardware and/or software will be required, whether responsibility for maintaining the hardware and/or software will be assumed by the agency or vendor, and a list of the non-law enforcement personnel who will be working on the project.
2. SLED will review the agency sponsor's letter and respond with a written approval to proceed. Additional clarification may be required before approval is granted. The approval notice will include instructions to the agency on the need for a Site Survey, required background investigations to consist at a minimum of criminal record checks on vendor personnel, and\or completion of a Security Addendum between the agency and the private vendor.
    a. If the vendor's product or service will alter the agency's existing network or security structure in any way, the agency must submit a revised Site Survey for approval. The Site Survey must indicate what those proposed changes will be.
    b. Any vendor personnel that will have contact with any un-encrypted NCIC data while working on the project must have background checks done on them before they will be permitted to access any SLED resources. Those record checks must be completed by the sponsoring agency and screened in accordance with the SLED NCIC Personnel Security Procedures.
    c. Any work done by a non-governmental private contractor on behalf of a criminal justice agency is subject to a Security Addendum. This addendum is to be incorporated as an extension of the contract made between the criminal justice agency and the private vendor. A copy of the completed addendum is to be forwarded by the criminal justice agency to SLED.
3. The sponsoring agency will complete and send to SLED any required Site Survey, security addendum, and statement verifying that background checks have been completed. The SLED Information Security Officer (ISO) will review and approve those documents. Written notice of that approval will be forwarded to the sponsoring agency.
4. If approved by the ISO, the vendor may then request copies of any published SLED documents it feels it needs to successfully complete the project. Assistance by SLED technical staff will only be provided to help clarify the material contained in those documents.
5. Due to time and personnel constraints, SLED technical support personnel will be unable to assist in debugging vendor code. All vendors are encouraged to provide their own tracing and debugging capabilities and not expect SLED to solve the problems.
6. Vendor testing will be allowed only from locations that are under the control of the sponsoring criminal justice agency. No remote dial-in or Internet access to SLED from vendor sites will be allowed.
7. SLED routinely audits and reports to sponsoring agencies all NCIC accesses for timeliness and accuracy. The sponsoring law enforcement agency is responsible for insuring that the vendor's solution complies with established guidelines.

8. Changes to NCIC or SLED data formats or procedural rules can be expected to occur in the future. SLED will communicate those changes directly to vendors as far in advance as possible to give vendors sufficient time to comply with those changes.

Appendix C

Security Requirements for Modems

This policy applies to all computers, whether dedicated or not to law enforcement, that reside on a network on which NCIC data passes.

No modems attached to individual PCs will be allowed to accept in-coming calls. All in-coming modem communications must be done by a RAS server protected by the perimeter firewall. It is highly recommended that a RAS server also be used to place out-going calls. In no case will the use of a modem on a networked PC be allowed to circumvent the protection afforded by the firewall.

Remote Access Servers (RAS) must be placed outside the firewall protecting law enforcement data. Firewall ports must be explicitly defined to allow communications between specific networked PCs and the RAS server.

RAS clients dialing into the server must be properly authenticated by the RAS server prior to gaining access to any other network device. The identity of the caller must be verified against a list of authorized users. Anonymous connections are not permitted.

All communication sessions must be encrypted using a minimum 128-bit key. In no cases will any un-encrypted NCIC data be allowed on a modem connection.

Modems attached to other network devices and used solely for remote service and support must be physically disconnected when not in use. Such modems must provide for proper authentication of the caller, use a hang-up and dial back facility to pre-defined phone numbers, provide encrypted communications with the caller, and be set to automatically timeout after 15 minutes of inactivity. Logging requirements are the same as those specified for RAS server access.

Each modem connection, whether successful or not, must be properly logged in a machine-readable log file. Logged information must include the date and time the connection attempt was made or RAS port was opened, the ID of the connecting user, any call-back number that was dialed, an indication of the success or failure to authenticate the user, and a timestamp showing when the connection was terminated. Log files must be kept available for auditing purposes for at least one calendar year.

Appendix D

Security Requirements for Wireless Access

Wireless access includes, but is not limited to, any fixed or mobile device that connects to a SLED data network. Authorization for wireless access to any SLED computer network may be granted by the Control Terminal Officer when a minimum set of technical and administrative requirements have been addressed to ensure the integrity of data and systems. In no case will wireless access be permitted without the prior approval of the SLED Control Terminal Officer.

Any wireless devices attaching to a SLED network must be properly secured to prevent unauthorized access or capturing of data streams. At a minimum, all wireless data communications must be protected using an encryption technique that employs a 128-bit key. The use of Wired Equivalent Privacy (WEP) is not sufficient to provide adequate security and is therefore not an acceptable level of protection.

No wireless access points or mobile data terminals will be installed without the prior, written approval of the Control Terminal Officer (CTO) or his designate. Requests for approval must be submitted in writing to the CTO and must include a description of where the wireless access will occur and the justification for it.

In no cases will the use of a wireless access point be allowed to circumvent the protection afforded SLED networks by firewalls or other protective devices.

Appendix E

Security Addendums and Background Checks

When is a security addendum required?

- No security addendum is needed for escorted emergency or occasional access
- SLED's Basic Security Addendum is needed for escorted, regular access by 3rd party contractors or service company employees
- FBI Security Addendum is needed for contractors that have un-escorted access

"Escorted" means personally accompanied into and out of the restricted location and under continuous control and supervision by an employee of the criminal justice agency or other government agency providing services to a criminal justice agency.

The Basic Security Addendum is executed between the criminal justice agency and the contractor or service company. A copy of the addendum must be forwarded to SLED.

The FBI Security Addendum is also executed between the criminal justice agency and the contractor company. All contractor employees who will have un-escorted access to NCIC data must initial it. A copy must be forwarded to SLED.

When are background checks required?

Fingerprint-based state and national checks must be done on any person having direct access to un-encrypted NCIC data. (Examples: CAD operators or 3rd party vendors developing software that accesses NCIC data.) This includes anyone that is subject to the FBI Security Addendum.

Name-based checks must be done on any person providing information systems support to the criminal justice agency where they might have incidental exposure to un-encrypted NCIC data. (Examples: county or city Information Technology employees, private contractors, or service companies that provide desktop hardware, software, or networking support.)

No background checks are required on systems support personnel that only come in contact with fully encrypted NCIC data. (Examples: personnel employed by companies that provide wide area networking circuits.)

Appendix F

Router Configuration Request

All routers that are being used to access the National Crime Information Center 2000 Computer System through the South Carolina Law Enforcement Criminal Justice Information Services (SLED CJIS) must be configured by SLED CJIS before being employed.

I , __________________________, am a representative of ________________________________ and hereby authorize the configuration of the following router(s) by SLED CJIS. SLED CJIS will not be held responsible for any existing router malfunctions.

			Please circle	
Company Make	**Model Number**	**Serial Number**	**Line Type**	
_Cisco___________	________________	________________	T-1	64k
_Cisco___________	________________	________________	T-1	64k
_________________	________________	________________	T-1	64k

Delivered by:

Name: ________________________________ Date: ________________________

Organization: ____

Address: ____

City: ____________________________, State: ____________________, Zip Code: ____________

Signature: ____ Phone: _______________________

Received by:

Name: ________________________________ Date: ________________________

SLED CJIS
4400 Broad River Road
Columbia, South Carolina 29210

Signature: ____

Returned and Installed by:

Name: ________________________________ Date: _________________________

SLED CJIS
4400 Broad River Road
Columbia, South Carolina 29210

Signature: ____

Received by:

Name: ________________________________ Date: ________________________

Signature: ____